Remarks

The application has been carefully reviewed in light of the Final Rejection, and the claims have been redrafted to more appropriately express the inventive concept disclosed and taught herein. Accordingly, the claims formerly in the case are all hereby cancelled and replaced with new claims 23 to 31. The main focus of the claims and the invention disclosed is the issue of the integrity of the auctioneer and how it is proved and demonstrated to the participants to their satisfaction. According to the new claims, the auction take place under circumstances whereby the integrity and faithfulness of the auctioneer is proved and verified by the way in which the auction proceeds and by the results. At the same time, the security of each participant is maintained and the auction proceeds in a highly secure way via a network. The result of the invention, as will be evident from the new claims, is that every participant has a way of verifying to herself, himself or itself that the auction is fair and the result is true and correct and the auctioneer is trustworthy, even though each participant only knows its inputs and is without any knowledge regarding the inputs of the other participants.

Independent claim 23 recites the method invention in terms that clearly distinguish the invention claimed from the cited prior art, and particularly distinguishes from U.S. Patent No. 5,905,975 to Ausubel ("Ausubel"). Ausubel discloses in great detail a computer implemented system and method of executing an auction, which allows flexible bidding by participants in a dynamic auction, combining some of the advantageous facets of a sealed-bid format with the basic advantages of an ascending-bid format, and the ability to bid on multiple objects. However, Ausubel does not disclose or teach any way to verify the trustworthiness of the auctioneer, which is the main thrust of the present invention.

New claim 23 is here set forth to demonstrate the critical manner in which the auctioneer's trustworthiness is verified to each participant. To this end, the limitations that particularly bear on the issue of the auctioneer's trustworthiness and the fact that the auction has been fairly done are placed in italics for emphasis.

23. (New) A method for preserving the integrity of a negotiation conducted via a

network, such as, the Internet, and using clients and/or servers, among a plurality of parties each of whom is making a private input during the negotiation and wherein a trusted entity acting as a center computes and outputs a value F of these inputs constituting the output of the negotiation comprising the steps of:

a) providing an architecture which includes a center A, and a plurality of participants B.sub.l, B.sub.2,..., B.sub.n, to engage in a negotiation during which all communications originating with a participant B.sub.i and transmitted to center A are exclusive;

b) secretly generating an input x.sub.i by each participant B.sub.i;

c) publishing by the center A to each participant a commitment to K combinatorial circuits that compute F, where K is a security parameter;

d) transmitting by each participant B.sub.i to the center A a commitment c.sub.i to the value of B.sub.i's input x.sub.i, where c.sub.i is an encryption of x.sub.i;

e) responsive to receipt of the commitments of the participants, publishing by the center A to the participants the commitments received;

f) providing to each participant B.sub.i part of the K combinatorial circuits that the center A committed to, and requesting center A to open them, whereupon each participant B.sub.i can verify that the part of the circuits opened to participant B.sub.i computes a value F;

g) transmitting by each participant B.sub.i to center A its input x.sub.i and decryption data to enable center A to verify that x.sub.i corresponds to the transmitted commitment c.sub.i;

h) computing by center A a value of F based on the inputs x.sub.i it received by using a part of the K combinatorial circuits not disclosed to the participants, and publishing the computed value of F to the participants; and

i) transmitting to all participants a proof that the computed value of F was computed correctly, which proof can be verified by each participant using the published commitments while preventing a coalition of any one subset of participants from learning (i) anything which cannot be computed just from the output of the K *combinatorial circuits and from their own inputs, and (ii) information about the inputs of other users.*

As stated above, the invention expressed by claim 23 contains a number of limitations (italicized) directed toward not only the auction but the verification and proof that the auction has been conducted fairly and the auctioneer has proved its trustworthiness. None of these italicized limitations can be found in Ausubel, nor are they disclosed, taught or even hinted at by Ausubel. More particularly, the limitation expressed in step c), to wit, *publishing by the center A to each participant a commitment to K combinatorial circuits that compute F, where K is a security parameter;* is completely novel with respect to Ausubel. The limitation expressed in step d) of transmitting a commitment (this is an encrypted bid which the center A cannot know at this point in the method) using encryption is completely novel with respect to Ausubel. The center A (which can be one entity or a group of entities) cannot know what the bid is at this point, and remains in the dark, so to speak, until the bid is made known to the center A in step g) upon receipt of the decryption data. The limitations of steps e) to i) of proceeding with the auction and proving its correctness and verifying the trustworthiness of the auctioneer are all completely novel with respect to Ausubel. Accordingly claim 23 is allowable. The same reasoning applies to independent claims 27 and 31, which recites critical limitations in the nature of those noted above. These claims 27 and 31 are also allowable. Claims 24 to 26 are dependent from claim 23 and contain all the limitations of claim 23, and accordingly are also allowable. Claims 28 to 30 are dependent from claim 27 and contain all the limitations of claim 27, and accordingly are also allowable.

The remaining prior art cited of record has been reviewed and all are more irrelevant that Ausubel, and none show or disclosed the claimed combinations of steps as recited in claims 23 to 31.

In light of the foregoing remarks, this application should be in condition for allowance, and early passage of this case to issue is respectfully requested. If there are any questions regarding this amendment or the application in general, a telephone call to the undersigned would be appreciated since this should expedite the prosecution of the application for all concerned.

A fee of $395 is believed to be due for a Request for Continued Examination. A PTO-2038 Credit Card Payment Form is submitted herewith. Please charge any additional fees (or credit any overpayment of fees) to the Deposit Account of the undersigned, Account No. 500601 (Docket No. 704-X99-043).

Respectfully submitted,

Martin Fleit

Martin Fleit, Reg. #16,900

Customer Number: 27317
Martin Fleit
FLEIT KAIN GIBBONS GUTMAN BONGINI & BIANCO, P.L.
21355 East Dixie Highway, Suite 115
Miami, Florida 33180
Tel: 305-830-2600; Fax: 305-830-2605
e-mail: mfleit@fleitkain.com